


<div><div>Es el momento de todos</div><div><div>Bancolombia</div></div></div>	<div>INSTALACIÓN, CONFIGURACIÓN Y ACTIVACIÓN DE SOFTWARE TOKEN EN WINDOWS</div>	Código:	MA-BCSI-SS-02
		Versión:	4
		Proceso / Negocio:	Bancolombia Seguridad Infraestructura
Este es un documento electrónicamente controlado y publicado. Para una impresión o copia física debe ser verificada o comparada con la versión electrónica antes de su uso.			

### 1. Objetivo

El propósito del documento es definir una guía práctica para la instalación, configuración y activación del software token en el sistema operativo Windows, a los usuarios de la organización Bancolombia.

### 2. Alcance

Este documento está diseñado para todos los empleados y proveedores que prestan servicios para el Grupo Bancolombia, conozcan el paso a paso para realizar la instalación, configuración y activación del software token en el sistema operativo Windows.

### 3. Definiciones

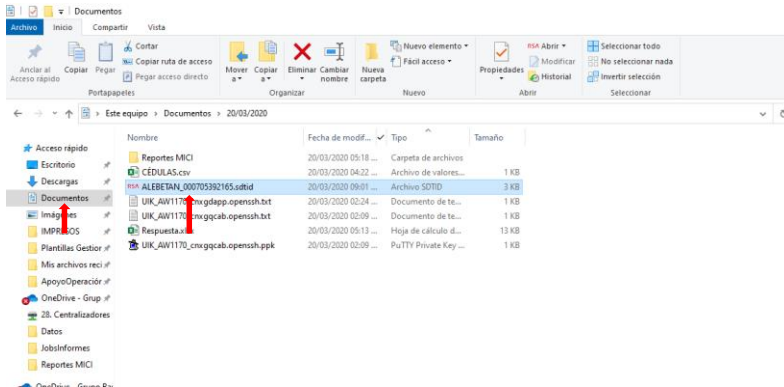
**RSA:** (Rivest, Shamir y Adleman) es un sistema criptográfico de clave pública desarrollado en 1977. Es el primer y más utilizado algoritmo de este tipo que es válido tanto para cifrar como para firmar digitalmente. La seguridad de este algoritmo radica en el problema de la factorización de números enteros.

**Software Token:** Software utilizado por la suite RSA SecureID para proveer la autenticación multifactorial, este software genera un número aleatorio de 8 dígitos cada minuto y puede instalarle en equipos de cómputo y dispositivos móviles.

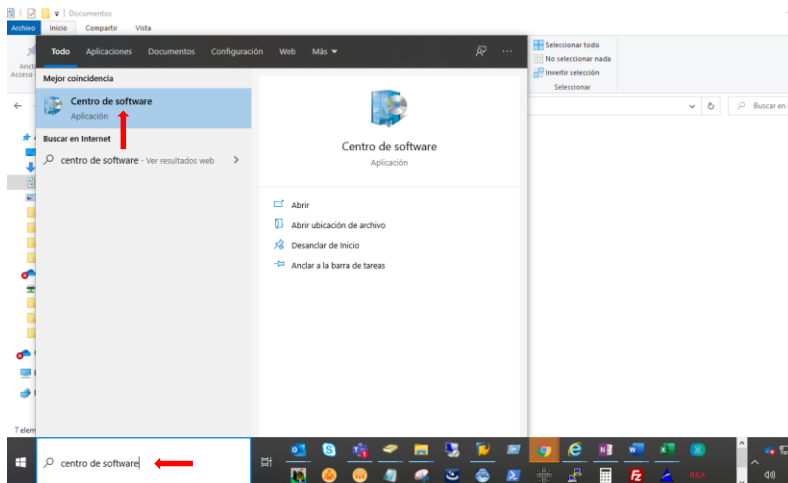
**RSA SecurID Software Token 5.0.2 for Windows:** Aplicación utilizada en equipos de escritorio y portátiles con sistema operativo Windows, que permite importar el software token para acceder a la VPN y otros recursos protegidos por RSA SecureID.

#### 4. Pasos para la activación del Software\_Token

- 4.1. Luego de haber descargado su software Token o Semilla en tu equipo (archivos adjunto al correo que termina en la extensión .sdtid).



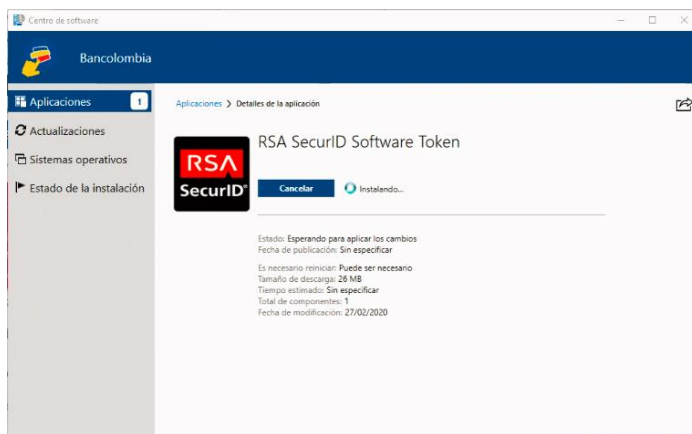
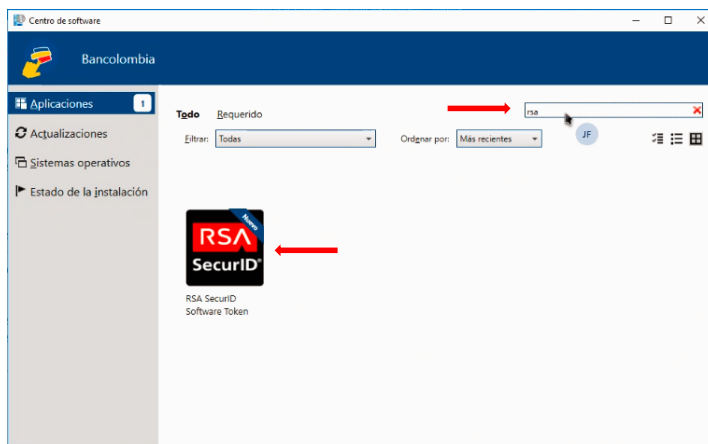
- 4.2. Procedemos con la instalación del Software Token, para esto, buscamos en el equipo "Centro de Software" y le damos clic,



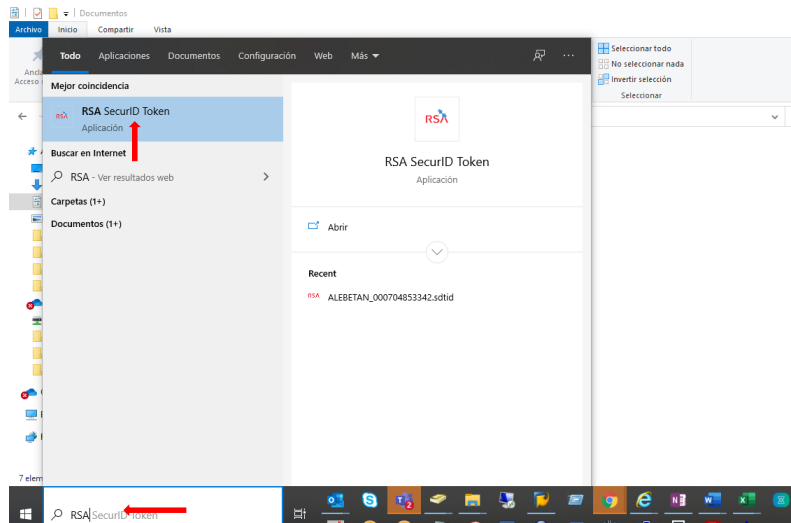
Comentado [W01]: el zip no va

- 4.3. Luego de abrir el Centro de Software, buscamos la aplicación “RSA”, seleccionamos el icono “RSA SecurID Software Token” y das clic en instalar.

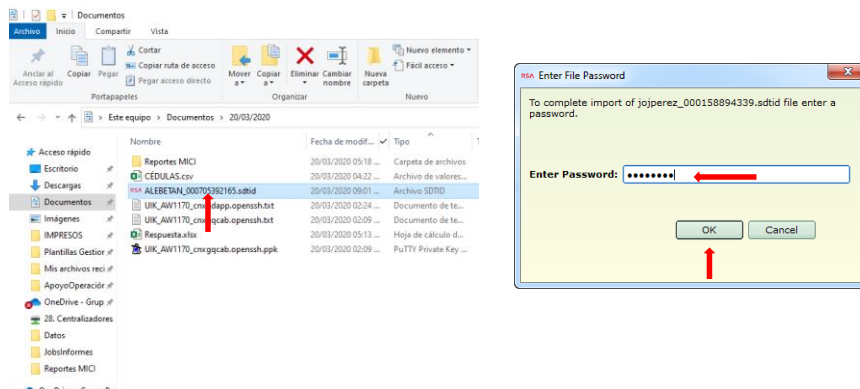
NOTA: la instalación está sujeta a que el equipo sea banco y hacerlo dentro de la red Banco, de lo contrario no le permitirá la instalación



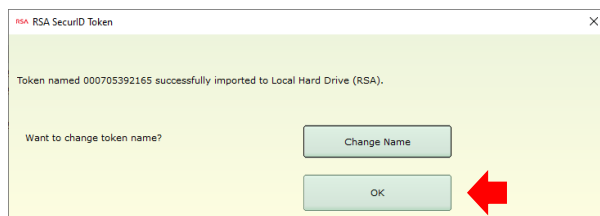
4.4 Una vez instalado, puedes cerrar la ventana del Centro de Software y luego buscar la palabra RSA en tu equipo, y abrir la aplicación “RSA SecurID Token”



4.5 Luego de abrir la aplicación RSA, debes buscar la ruta donde guardo el Software\_Token o semilla (el archivos que guardo en sus documentos que termina en .sdtid). Le das doble clic para abrirlo, allí te pedirá que ingreses la contraseña que te fue enviada en el correo con la semilla y luego dar OK.

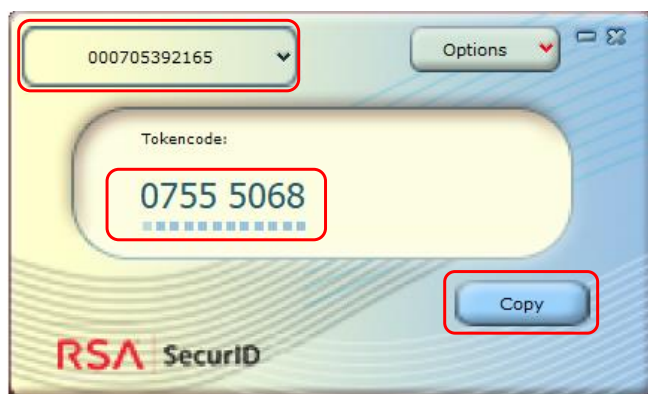


#### 4.6 Damos OK para culminar la configuración del Software Token



5. De esta forma finaliza la instalación del software token y en la pantalla principal se pueden visualizar los siguientes datos:

1. **Serial del Software Token:** Número de la parte superior izquierda, el cual es útil conocerlo al momento de requerir algún tipo de soporte por parte de la mesa de ayuda Mateo (Desbloqueo Token, Clareo de PIN, entre otros procesos).
2. **Tokencode:** Número que cambia cada 60 segundos el cual, junto con el PIN, forma el Passcode que es requerido para acceder a los diferentes sistemas del BANCO.
3. **Botón COPY:** Hacemos uso de la funcionalidad de este botón para copiar los 8 dígitos actuales del token, que corresponden al Tokencode.



## 6. Activación del software token

La activación del software token, tiene exactamente el mismo proceso que el de un token físico el cual se describe a continuación.

- o Acceder a: <https://accesoremoto.bancolombia.com>, allí, ingresas los siguientes datos:

**Nombre de Usuario:** Usuario de red banco

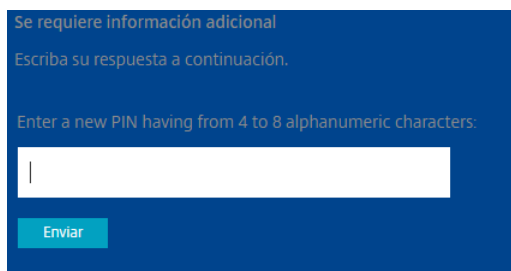
**Contraseña:** Contraseña de red banco

**Passcode:** Ingresar **solo** los 8 dígitos Alfanuméricos que aparecen en la pantalla de tu Software\_Token, esto se hace por única vez.

Luego Das clic en Iniciar Sesión.



- o En la siguiente ventana solicita ingresar un PIN de 4 a 8 dígitos alfanuméricos (se recomienda que sea de 4 dígitos numéricos para fácil recordación), este PIN es complemento del TokenCode y juntos conforman el PASSCODE (PIN + TokenCode), el cual será utilizado siempre que se requiera acceder con token luego de la activación de este.



- o Luego de ingresar y confirmar el PIN, se solicitará el PASSCODE.

**PASSCODE:** Es la combinación del PIN creado + Tokencode

**PIN:** Es fijo, creado por el usuario, debe ser seguro, pero de fácil recordación.

**Tokencode:** Secuencia de 8 números que da el Software Token, no requiere recordación, ya que este cambia cada 60 segundos.

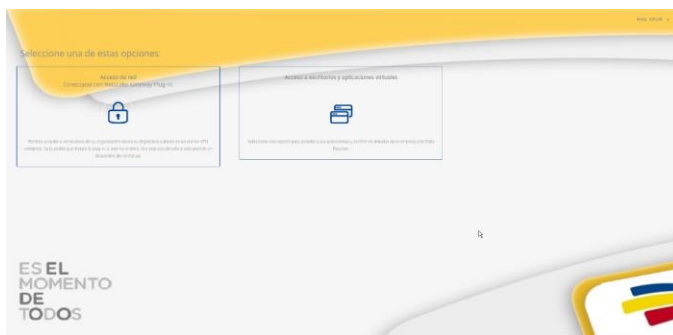
Se requiere información adicional

Escriba su respuesta a continuación.

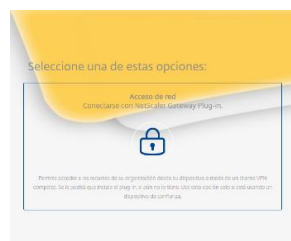
Please Enter Passcode

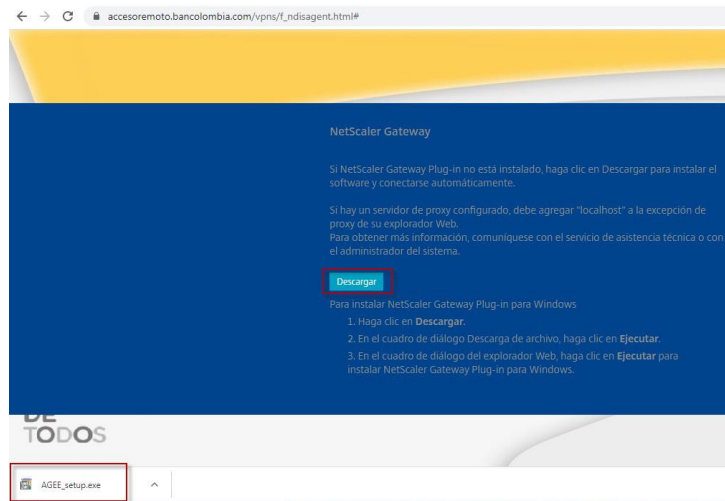
Enviar

- Una vez ingresado el Passcode, logras acceder a la VPN y el Token queda activado saliendo la siguiente venta, donde podrás seleccionar trabajar con **VPN** (aplicaciones instaladas en tu equipo y con los permisos requeridos previamente en el grupo VPN) o con **Aplicaciones** virtualizadas (aplicaciones configuradas previamente y que debes tener los grupos asociados)



- Si seleccionas la primera opción que es VPN, te saldrá la opción de descargar un plugin para que sea instalado en tu portátil.





**NOTA:** En caso de que te pida descargar el Plugin de Citrix, este no podrá ser instalado si te encuentra por fuera de las instalaciones del banco, procurar instalarlo estando en red banco y con apoyo de MATEO ya que pide que seas Administrador de tu maquina

Recuerda que si requieres ayuda con esta configuración debes apoyarte con la Mesa de Servicios Mateo.

#### 4. Documentos Asociados

N/A.

#### 5. Riesgos del proceso

Personal no idóneo  
Uso inadecuado de la información  
Pérdida o robo de información

#### 6. Seguridad de la Información

Todo el personal de Axity, deberá cumplir con los procedimientos y políticas de Seguridad de la Información de la compañía, establecidas en el sistema de Gestión.  
Teniendo en cuenta esta información, este documento es considerado de uso interno en la organización.

#### 8. Control de Cambios

Identificar los criterios mencionados a continuación.



Versión	Fecha	Responsable Nombre / Cargo	Cambio realizado
1	30/11/2017	Jonathan Andres Betancur Arredondo	Creación del documento
2	20/08/2019	Luis Fernando Lopera Gómez	Actualización del Documento
3	24/09/2019	Úrsula Arias Lotero	Verificación y aprobación del documento
4	01/12/2019	Manuel Toro Velez	Actualización del Documento
5	20/03/2020	Alexander Betancur Martínez Walther Cifuentes Osorio Andres Camilo Rivera	Actualización del Documento